DANE – DNS Based Authentication of Named Entities

August 2016

Mark Elkins

DNS-Based Authentication of Named Entities - RFC 6698

Allows the storage of SSL/TLS Certificates or Certificate "fingerprints" as a (TLSA) DNS Record.

Prerequisites:

1 - The Domain needs to be DNSSEC signed - with a valid chain of trust
This is to prove that the zone contents are authentic
and have not been tampered with in any way.

2 - There needs to be a suitable SSL/TLS Certificate for the Website or Mail System for this Domain.

A Wildcard for the Domain "*.virtual.web.za" may simplify administration
The SSL/TLS Certificate can come from any Certificate Authority (CA) or for use with just e-mail, be self signed.

DNS
DOMAIN NAME SERVICES

Websites

Problem: It is possibility that a SSL/TLS Certificate Authority is compromised.

Solution: Add a Fingerprint.

The Fingerprint in the DNS must match the certificate found

Recommendation: TLSA 3 0 1 Record

3 - Certificate Usage - Match a specific certificate
0 - Selector - The Full certificate (including expiry Date)
1 - Matching Type - SHA-256 hash of selected content

DNS
DOMAIN NAME SERVICES

Websites

Create:

cat virtual.web.za.crt | openssl x509 -outform DER | openssl sha256
-or-
openssl s_client -connect virtual.web.za:443 | openssl x509 -outform der | \
openssl sha256

To test - add:

_443._tcp.virtual.web.za. IN TLSA 3 0 1 a2d3c395f8d2f2c4416cf...

to the DNS Zone (in this case) virtual.web.za

DNS
DOMAIN NAME SERVICES

Websites

Add the plugin "DNSSEC Validator" to your Browser

Validation processing is done by looking up all TLSA records that match the Web Site, that is the port (443) and Name (virtual.web.za). There may be multiple TLSA records, only one needs to match.

_443._tcp.virtual.web.za. IN TLSA 3 0 1 a2d3c395f8d2f2...

DNS
DOMAIN NAME SERVICES

Websites

Certificate Roll-over process

SSL/TLS Certificates are often valid for two or three years.
On change, recreate TLSA, add to DNS.
Once propagated, deploy new SSL/TLS Certificate.

Effort and Reward

Most Effort, learning how to create TLSA record.
Trivial to keep up to date, only change on Certificate changes.
Possible to automate.

Reward is providing the Customer with more confidence that they have connected with the correct Web Server.

DNS
DOMAIN NAME SERVICES

Mail Servers

As with Web servers, the DNS Fingerprint for the Mail Server must match the Mail Servers certificate.

Recommendation: TLSA 3 1 1 Record

3 - Certificate Usage - Match a specific certificate
1 - Selector - SubjectPublicKeyInfo, DER-encoded binary structure,
no Date meta-info
1 - Matching Type - SHA-256 hash of selected content

DNS
DOMAIN NAME SERVICES

Mail Servers

Created by:

```
cat virtual.web.za.crt | openssl x509 -noout -pubkey | \
      openssl pkey -pubin -outform DER | openssl sha256
```

Deploy as:

```
_25._tcp.mail.virtual.web.za.  IN TLSA 3 1 1 14953f181db94724557...
```

in the DNS Zone (in this example) virtual.web.za

Validation process: done by looking up all matching TLSA records.
There may be multiple TLSA records, only one needs to match.
EXIM and POSTFIX can use these records.

DNS
DOMAIN NAME SERVICES

Mail Servers

Effort and Reward:

Most **Effort** spent on learning.
Trivial to keep up to date.
Only necessary whenever the CSR (Certificate Request) changes.

Change may never happen, so remember, fully document where, why and how to reproduce.

Reward: providing connection confidence and security.

German ISP's, promote their services as being more secure.

DNS
DOMAIN NAME SERVICES

Mail Servers

Effort and Reward:

Until now, no signalling method for Mail Server using Certificates.
Mail Servers tend to be opportunistic in using TLS.
Allows for Man-in-the-middle attacks.

TLSA Records for Mail Servers *like* HTTPS for Web servers

The Record Implies - Only connect using TLS encryption.
(Transport Layer Security)

The SSL/TLS certificate must match the TLSA fingerprint.
No Match → No connection.

DNS
DOMAIN NAME SERVICES

Get in Touch

Mark Elkins
mark@dns.net.za
www.dns.net.za
Twitter: @dns_africa
Facebook: Domain Name Services

DNS
DOMAIN NAME SERVICES